Computing modular Galois representations

Nicolas Mascot
IMB, Université Bordeaux 1
nmascot@math.u-bordeaux1.fr

November 20, 2012

Abstract

We compute modular Galois representations associated with a newform f, and study the related problem of computing the coefficients of f modulo a small prime ℓ. To this end, we design a practical variant of the complex approximations method presented in [EC11]. Its efficiency stems from several new ingredients. For instance, we use fast exponentiation in the modular jacobian instead of analytic continuation, which greatly reduces the need to compute abelian integrals, since most of the computation handles divisors. Also, we introduce an efficient way to compute arithmetically well-behaved functions on jacobians. We illustrate our method on the newform Δ, and manage to compute for the first time the associated faithful representation modulo ℓ and the values modulo ℓ of Ramanujan's τ function at huge primes for $\ell \in \{11, 13, 17, 19\}$. In particular, we get rid of the sign ambiguity stemming from the use of a non-faithful representation as in [Bos07].

Acknowledgements

I would like to heartily thank my advisor J.-M. Couveignes for offering me this beautiful subject to work on. More generally, I would like to thank people from the Bordeaux 1 university's IMB for their support, with special thoughts to B. Allombert, K. Belabas, H. Cohen and A. Enge, as well as the PlaFRIM team. Finally, I thank A. Page for helping me to make explicit the similarity classes in $GL_2(\mathbb{F}_\ell)$, and T. Selig for proofreading my English.

1 Introduction

Consider a newform $f = q + \sum_{n\geqslant 2} a_n q^n \in S_k\big(\Gamma_1(N)\big)$ of weight k and level $N \in \mathbb{N}^*$. Attached to it is a system of Hecke eigenvalues $\lambda_f \colon \mathbb{T}_{k,N} \longrightarrow \mathbb{Z}_{K_f}$, namely

$$Tf = \lambda_f(T)f, \quad T \in \mathbb{T}_{k,N},$$

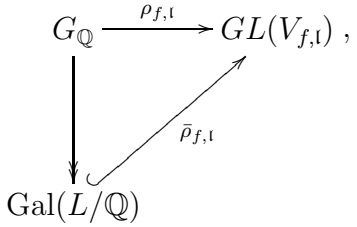
where $\mathbb{T}_{k,N} = \mathbb{Z}[T_n,\, n \geqslant 2]$ denotes the Hecke algebra acting on cuspforms of weight k and level N, and where $\mathbb{Z}_{K_f}$ is the ring of integers of the number field $K_f = \mathbb{Q}(a_n, n \geqslant 2)$ of f. Let $\mathfrak{l}$ be a prime of inertia degree 1 of K_f, lying above a rational prime $\ell \geqslant k-1$ which does not divide N. Reducing modulo $\mathfrak{l}$, we get a ring morphism $\lambda_{f,\mathfrak{l}} \colon \mathbb{T}_{k,N} \longrightarrow \mathbb{F}_\ell$. By level-lowering theorems (cf [Rib94] for $\ell > 2$ and [Buz00] for $\ell = 2$), there exists another ring morphism $\mu_{f,\mathfrak{l}} \colon \mathbb{T}_{2,\ell N} \longrightarrow \mathbb{F}_\ell$ such that $\lambda_{f,\mathfrak{l}}(T_p) = \mu_{f,\mathfrak{l}}(T_p) \in \mathbb{F}_\ell$ for all rational primes p. This other Hecke algebra $\mathbb{T}_{2,\ell N}$ also acts on the jacobian $J_1(\ell N)$ of the modular curve $X_1(\ell N)$, so let us consider the subspace

$$V_{f,\mathfrak{l}} = \bigcap_{T\in\mathbb{T}_{2,\ell N}} \mathrm{Ker}\,\big(T - [\mu_{f,\mathfrak{l}}(T)]\big)\big|_{J_1(\ell N)[\ell]}$$

of the ℓ-torsion part of $J_1(\ell N)$. One shows (cf [Edi92], theorem 9.2) that $V_{f,\mathfrak{l}}$ has dimension 2 as a vector space over $\mathbb{F}_\ell$ except[1] for a finite number of $\mathfrak{l}$, and that it is defined over $\mathbb{Q}$ (cf [DS05], section 7.9). We thus get a Galois representation

$$\rho_{f,\mathfrak{l}} \colon G_{\mathbb{Q}} \longrightarrow GL(V_{f,\mathfrak{l}}) \simeq GL_2(\mathbb{F}_\ell),$$

which is unramified outside ℓN (cf [DS05], theorem 9.6.5). Let $L = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\rho_{f,\mathfrak{l}}}$ denote the field cut out by this representation. We have the following diagram:



[1] It is the case if $\ell > k$ and the associated Galois representation is irreducible, which is the case except for finitely many $\mathfrak{l}$. We will exclude those cases from now on. In particular, when we work with $f = \Delta$, this implies we have to exclude $\ell = 23$ ([EdiC1], top of page 5), cf the last sentence in our results section.

where we denote with an extra bar the induced representation

$$\bar{\rho}_{f,\mathfrak{l}}\colon \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow GL(V_{f,\mathfrak{l}}).$$

Furthermore, it follows from the Eichler-Shimura relation (cf [DS05], theorem 8.7.2) that for $p \nmid \ell N$, the image of the Frobenius element $\left(\frac{L/\mathbb{Q}}{p}\right)$ by $\bar{\rho}_{f,\mathfrak{l}}$ has characteristic polynomial

$$X^2 - a_p X + \varepsilon(p)p^{k-1} \in \mathbb{F}_\ell[X],$$

where a_p denotes the p-th coefficient in the q-expansion of the newform f, ε is the Dirichlet character of f, and both have been reduced modulo $\mathfrak{l}$. Consequently, the knowledge of the Galois representation $\rho_{f,\mathfrak{l}}$ allows us to recover the coefficients of the q-expansion of f modulo $\mathfrak{l}$.

It would be interesting to compute explicitly these Galois representations $\rho_{f,\mathfrak{l}}$, for several reasons: first, simply for the sake of the Galois representation itself, next, because the number field L will often be an explicit solution to the inverse Galois problem for $GL_2(\mathbb{F}_\ell)$ (cf [Bos07a], [Bos11]), and, last but not least, because it gives a fast way of computing the q-expansion coefficients a_p of f modulo $\mathfrak{l}$. Letting ℓ vary, we thus obtain a Schoof-like algorithm (cf [Sch95]) to compute q-expansions of newforms, as bounds on the coefficients a_p are well-known.

Computing these representations is the goal pursued by the book [EC11]. The idea is to approximate ℓ-torsion divisors representing the points of $V_{f,\mathfrak{l}}$. To compute these torsion divisors, the book [EC11] suggests two approaches: a probabilistic one ([CouC13], chapter 13), which creates ℓ-torsion divisors by applying Hecke operators to random divisors on the modular curve over small finite fields, and a deterministic one ([CouC12], chapter 12), which relies on fast exponentiation to create approximations of torsion divisors on the modular curve over $\mathbb{C}$. However, neither of these two methods is practical at all, although their theoritical complexities are polynomial in ℓ.

In [Bos07], J. Bosman presents a practical variant of the complex method. It uses an analytic continuation method (cf for instance [Li03]) instead of fast exponentiation. To deal with the Abel-Jacobi map

$$\jmath\colon \mathrm{Div}^0\left(X_1(\ell N)\right)(\mathbb{C}) \to J_1(\ell N)(\mathbb{C}),$$

J. Bosman has to compute a lot of abelian integrals. This leads to precision issues as this requires summing q-series very close to the edge of the convergence disk, and because of the singular locus of $\jmath$, of which little is known.

J. Bosman still manages to compute representations up to level 17 and 19, but he only gets projective Galois representations in $PGL_2(\mathbb{F}_\ell)$ instead of $GL_2(\mathbb{F}_\ell)$, which means he gets the coefficients $a_p \bmod \mathfrak{l}$ up to a sign only (cf for instance the table on the very first page of [EC11]).

To our understanding, the implementation [Zen12] by J. Zeng of the probabilistic method suffers from the same limitations. J. Zeng computes polynomials defining projective non-faithful representations, but seems not to compute actual coefficients.

In this paper, we present another improved, practical and deterministic version of the complex approximations approach, which is provable in that the singular locus of $\jmath$ is no longer a problem. It has far fewer precision issues, as it computes abelian integrals only along very short paths well inside the convergence disks, and uses K. Khuri-Makdisi's algorithms [KM04] [KM07] for fast exponentiation in the jacobian. Consequently, we get approximations of torsion divisors fairly easily. In the last step, to increase the precision, we can use Newton iteration simply on the condition $[\ell]D \simeq 0$, instead of $\jmath(D) = x$ for some $x \in J_1(\ell N)[\ell]$. This allows us to compute the full Galois representations for the levels 17 and 19. As a consequence, we can for instance find the signs which were missing in J. Bosman's results. Furthermore, we believe that an optimisation of our code would allow us to compute representations in higher levels 29 and even 31, which has never been done yet. We give a detailed description of our method in the following sections of this paper.

Like J. Bosman, we limit ourselves to prime levels ℓ for commodity[2]. This implies that we can only use our algorithm to compute Galois representations attached to newforms of weight 2 and level ℓ, or to newforms of any weight but of level 1. Typically, we use it on the newform Δ, which is of weight 12 and level 1. As the genus of $X_1(\ell)$ is $g = \frac{(\ell-5)(\ell-7)}{24}$ for $\ell \geqslant 11$ and is 0 for $\ell \leqslant 7$, we will assume $\ell \geqslant 11$ throughout this paper.

In the next section, we present a quick review of our algorithm. Then, in section 3, we give a detailed description of the key steps. Finally, in the last section, we present actual computations of a Galois representation and of coefficients of a newform, and we give complexity estimates.

[2]However, we think our algorithm could easily be extended to general levels N.

2 Outline of the algorithm

Our first task consists in computing the period lattice Λ of $X_1(\ell)$, which we do by integrating cuspforms along modular symbols. Using our knowledge of the action of the Hecke algebra on modular symbols, we then deduce an analytic representation of the ℓ-torsion subspace $V_{f,\mathfrak{l}} \subset J_1(\ell)(\mathbb{C}) = \mathbb{C}^g/\Lambda$. Next, we find a way to invert the Abel-Jacobi map $\jmath$, so that we may, for each $x \in J_1(\ell)(\mathbb{C})$, find a null-degree divisor D_x on X such that $\jmath(D_x) = x$, and especially so for two ℓ-torsion divisor classes x_1 and x_2 forming a basis of the two-dimensional $\mathbb{F}_\ell$-subspace $V_{f,\mathfrak{l}}$.

We first compute the period lattice Λ by computing a $\mathbb{Z}$-basis of the singular homology $H_1\big(X_1(\ell)(\mathbb{C}), \mathbb{Z}\big)$ made up of modular symbols (cf [Ste07] or [Cre97]), along which we integrate term-by-term the q-expansions of a basis $(f_i)_{1\leqslant i\leqslant g}$ of cuspforms of weight 2. Now, by computing the Hecke action on $J_1(\ell)[\ell]$, we can express our two divisor classes x_1 and x_2 as points of $\frac{1}{\ell}\Lambda/\Lambda \subset \mathbb{C}^g/\Lambda$. We lift them to (as-short-as-possible) vectors $\widetilde{x_1}$, $\widetilde{x_2} \in \mathbb{C}^g$. Next, we choose $2g$ pairs of points $(P_n, P'_n)_{1\leqslant n\leqslant 2g}$, with each P'_n very close to P_n, and we compute their "Abel-Jacobi" images

$$p_n = \left(\int_{P_n}^{P'_n} f_i(\tau)d\tau\right)_{1\leqslant i\leqslant g} \in \mathbb{C}^g,$$

where for each n the integration path from P_n to P'_n is naturally chosen as a very short[3] path joining P_n to the very close point P'_n. Consequently, the vectors p_n will be very short. Moreover, we choose the pairs (P_n, P'_n) so that the vectors p_n span $\mathbb{C}^g$ over $\mathbb{R}$ in a not-too-ill-conditioned way, which is possible as there are $2g$ of them; we can thus express our points $\widetilde{x_k}$ as $\mathbb{R}$-linear combinations of the p_n,

$$\widetilde{x_k} = \sum_{n=1}^{2g} t_{n,k}p_n, \quad t_{n,k} \in \mathbb{R},\ k = 1, 2.$$

Now, as the p_n are very short, the coefficients $t_{n,k}$ are very large, so that we still have a reasonably good approximation

$$\widetilde{x_k} \approx \sum_{n=1}^{2g} \lfloor t_{n,k} \rceil p_n, \quad k = 1, 2,$$

[3]For instance, P'_n will be in the same coordinate chart as P_n, and we naturally choose a path which stays inside this coordinate chart.

where $\lfloor \cdot \rceil$ stands for the nearest integer. Consequently, the divisor

$$D_k^{\mathrm{big}} = \sum_{n=1}^{2g} \lfloor t_{n,k} \rceil \big((P'_n) - (P_n) \big)$$

will map by the Abel-Jacobi map to a reasonable approximation of $\widetilde{x_k}$. However, it has large coefficients, so we use K. Khuri-Makdisi's algorithms [KM04] [KM07] to reduce it, that is to say we compute an effective divisor D_k^{crude} of degree $d_0 = 2g+1$ such that $D - D_0$ is linearly equivalent to D_k^{big}, where D_0 is another effective divisor of degree d_0 used as an origin.

This way, we find approximations of ℓ-torsion divisors using only integrals along the short paths p_n, which are well inside the convergence disks. Consequently we have far fewer precision issues than with J. Bosman's method [Bos07].

We next refine these approximations using Newton iteration on the equation $\ell(D - D_0) \sim 0$. We thus get two ℓ-torsion divisors D_1^{fine} and D_2^{fine} whose images by the Abel-Jacobi map form a basis of the ℓ-torsion subspace $V_{f,\mathfrak{l}}$. We then compute all the reduced divisors

$$D_{a,b} \sim a D_1^{\mathrm{fine}} + b D_2^{\mathrm{fine}}, \quad a, b \in \mathbb{F}_\ell,$$

yielding a collection of ℓ^2 reduced divisors corresponding to the ℓ^2 points of $V_{f,\mathfrak{l}}$, and evaluate them by a well-chosen Galois-equivariant map $\alpha \colon V_{f,\mathfrak{l}} \longrightarrow \overline{\mathbb{Q}}$. The polynomial

$$F(X) = \prod_{\substack{a,b \in \mathbb{F}_\ell \\ (a,b) \neq (0,0)}} \big(X - \alpha(D_{a,b}) \big)$$

then lies in $\mathbb{Q}[X]$; we can recognise its coefficients using continued fractions. This polynomial encodes the Galois representation we are attempting to compute, in that its splitting field L over $\mathbb{Q}$ is the number field cut out by the representation $\rho_{f,\mathfrak{l}}$, and $\mathrm{Gal}(L/\mathbb{Q})$ acts on its roots $\varphi(D_{a,b})$ just like $GL_2(\mathbb{F}_\ell)$ acts on $(a,b) \in \mathbb{F}_\ell^2$.

Our final task consists is to describe the image of Frobenius elements by this representation. For this, we adapt T. and V. Dokchitser's work [Dok10] to get resolvents

$$\Gamma_C(X) \in \mathbb{Q}[X], \quad C \text{ similarity class of } GL_2(\mathbb{F}_\ell)$$

such that

$$\bar{\rho}_{f,\mathfrak{l}}\left(\left(\frac{L/\mathbb{Q}}{p}\right)\right) \in C \iff \Gamma_C\big(\operatorname{Tr}_{A_p/\mathbb{F}_p} a^p\, h(a)\big) = 0 \bmod p,$$

where $A_p = \mathbb{F}_p[X]/\big(F(X)\big)$, a denotes the class of X in A_p, and h is a polynomial (cf [Dok10] or the relevant part of the next section).

Finally, we can now compute the coefficients a_p of the q-expansion of f modulo $\mathfrak{l}$:

$$a_p \bmod \mathfrak{l} = \operatorname{Tr} \bar{\rho}_{f,\mathfrak{l}}\left(\left(\frac{L/\mathbb{Q}}{p}\right)\right).$$

3 Detailed description of the steps

We first show in subsection 3.1 how to efficiently compute the period lattice of $X_1(\ell)$. Then, we explain in 3.2 how to use K. Khuri-Makdisi's algorithms [KM04] [KM07] on $X_1(\ell)$; our method requires carefully chosing Eisenstein series, as explained in 3.3. After this, we show in 3.4 how to use these algorithms to reduce a big divisor sum, and in 3.5 we explain how to use Newton iteration to refine the result into ℓ-torsion. Finally, we explain in 3.6 how to construct a well-behaved function on the jacobian $J_1(\ell)$ and how to evaluate it at the ℓ-torsion divisors, and we conclude by describing in 3.7 an efficient way of computing the image of the Frobenius elements by the Galois representation.

3.1 Computing the periods of $X_1(\ell)$

Computing the period lattice Λ amounts, by the Manin-Drinfeld theorem (cf [Lan95], chapter IV, theorem 2.1), to compute integrals of newforms of weight 2 along modular symbols, such as

$$\int_{\infty}^{0} f(\tau) d\tau.$$

These integrals can be computed by integrating q-expansions term by term. However, we have to split the integration path so that the resulting series converges. Furthermore, to increase the convergence speed, we need the path ends to lie well-inside the convergence disks.

To reduce the number of integrals we compute, we use the adjointness property of the Hecke operators with respect to the integration pairing between modular symbols and cuspforms. In general, the modular symbol $\{\infty, 0\}$ alone does not span the rational homology of the modular curve, even over $\mathbb{T}_{2,\ell} \otimes \mathbb{Q}$, so we introduce other modular symbols, the twisted winding elements w_p.

More precisely, define (cf [BosC6], section 6.3), for any $p \neq \ell$ prime or $p = 1$, the twisted winding element

$$w_p = \sum_{a \bmod p} \left(\frac{a}{p}\right) \left\{\infty, \frac{a}{p}\right\} \in \mathbb{M}_2\big(\Gamma_1(\ell)\big),$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, which we define to be 1 if $p = 1$ for convenience. We write each basis element γ_j of $H_1\big(X_1(\ell)(\mathbb{C}), \mathbb{Z}\big)$ as a $\mathbb{T}_{2,\ell} \otimes \mathbb{Q}$-linear combination

$$\gamma_j = \sum_p T_{j,p} w_p, \quad T_{j,p} \in \mathbb{T}_{2,\ell} \otimes \mathbb{Q}.$$

We can compute the periods using the adjointness property of the integration pairing with respect to Hecke operators as follows:

$$\int_{\gamma_j} f(\tau)d\tau = \int_{\sum_p T_{j,p} w_p} f(\tau)d\tau = \sum_p \int_{w_p} (T_{j,p} f)(\tau)d\tau = \sum_p \lambda_{j,p} \int_{w_p} f(\tau)d\tau,$$

where $\lambda_{j,p} \in \mathbb{C}$ denotes the eigenvalue of the newform f for the Hecke operator $T_{j,p}$.

Consequently, all we need is to compute the integrals $\int_{w_p} f(\tau)d\tau$. Given a cuspform

$$f = \sum_{n \geqslant 1} a_n q^n \in S_2\big(\Gamma_1(\ell)\big),$$

and χ a Dirichlet character modulo $p \neq \ell$, one defines the twisted cuspform[4]

$$f \otimes \chi = \sum_{n \geqslant 1} a_n \chi(n) q^n.$$

[4]Indeed, twisting by a Dirichlet character whose modulus is prime to the level preserves cuspforms, though it raises the level, cf [AL78], proposition 3.1.

It is a cuspform of level ℓp^2. The Fricke involution W_ℓ transforms the form $f(\tau)$ into $\frac{1}{\ell\tau^2} f\left(\frac{-1}{\ell\tau}\right)$. It is useful for our purpose in that it can be used to move a τ with small imaginary part to $\frac{-1}{\ell\tau}$, which can have a much larger imaginary part. We read in [BosC6], section 6.2, that if $f = q + \sum_{n\geqslant 2} a_n q^n \in S_2\big(\Gamma_1(\ell), \varepsilon\big)$ is a newform with weight 2, level ℓ and character ε, then $W_\ell f$ is the newform with weight 2, level ℓ and conjugate character $\overline{\varepsilon}$ defined by

$$W_\ell f = \lambda_\ell(f) \left(q + \sum_{n\geqslant 2} \overline{a_n} q^n \right),$$

where $\lambda_\ell(f)$ is given by

$$\lambda_\ell(f) = \begin{cases} -\overline{a_\ell} & \text{if } \varepsilon \text{ is trivial,} \\ \dfrac{g(\varepsilon)\overline{a_\ell}}{\ell} & \text{if } \varepsilon \text{ is nontrivial,} \end{cases}$$

where $g(\cdot)$ denotes the Gauss sum of a Dirichlet character. Moreover, if f is a newform of weight 2 with character ε, one has the formula

$$W_{\ell p^2}(f \otimes \chi) = \frac{g(\chi)}{g(\overline{\chi})} \varepsilon(p)\chi(-\ell) \cdot (W_\ell f) \otimes \overline{\chi}.$$

An easy computation shows that

$$\sum_{a \bmod p} \overline{\chi}(a) f(\tau + a/p) = g(\overline{\chi})(f \otimes \chi)(\tau).$$

This yields the formula

$$\int_{w_p} f(\tau)d\tau = g\left(\left(\frac{\cdot}{p}\right)\right) \int_\infty^0 \left(f \otimes \left(\frac{\cdot}{p}\right)\right)(\tau)d\tau$$

$$= g\left(\left(\frac{\cdot}{p}\right)\right) \left(\int_\infty^{\frac{i}{p\sqrt{\ell}}} \left(f \otimes \left(\frac{\cdot}{p}\right)\right)(\tau)d\tau + \int_{\frac{i}{p\sqrt{\ell}}}^0 \left(f \otimes \left(\frac{\cdot}{p}\right)\right)(\tau)d\tau \right)$$

$$= g\left(\left(\frac{\cdot}{p}\right)\right) \left(\int_\infty^{\frac{i}{p\sqrt{\ell}}} \left(f \otimes \left(\frac{\cdot}{p}\right)\right)(\tau)d\tau - \int_\infty^{\frac{i}{p\sqrt{\ell}}} W_{\ell p^2}\left(f \otimes \left(\frac{\cdot}{p}\right)\right)(\tau)d\tau \right)$$

$$= \frac{g\left(\left(\frac{\cdot}{p}\right)\right)}{2\pi i} \sum_{n=1}^{+\infty} \left(a_n - \varepsilon(p)\left(\frac{-\ell}{p}\right)\lambda_\ell(f)\overline{a_n} \right) \frac{\left(\frac{n}{p}\right)}{n} \left(e^{-\frac{2\pi}{p\sqrt{\ell}}}\right)^n,$$

which allows us to compute the integral of a newform along a twisted winding element, and thus to finally compute the period lattice of the modular curve $X_1(\ell)$. We sum power series at $q = e^{-\frac{2\pi}{p\sqrt{\ell}}}$ for small primes p[5], which has small enough modulus to achieve fast convergence.

3.2 Arithmetic in the jacobian $J_1(\ell)$

In order to efficiently compute in the jacobian $J_1(\ell)$, we use K. Khuri-Makdisi's algorithms [KM04] [KM07]. This requires choosing an effective divisor D_0 of degree $d_0 \geqslant 2g+1$ such that we know how to compute the associated complete linear series

$$V = H^0\big(X_1(\ell), 3D_0\big).$$

A divisor class $x \in J_1(\ell)$ is then represented by an effective divisor D of degree D_0 such that the class of $D - D_0$ is x, and D is itself represented by the subspace

$$W_D = H^0\big(X_1(\ell), 3D_0 - D\big) \subset V;$$

in particular $0 \in J_1(\ell)$ can be represented by

$$W_0 = H^0\big(X_1(\ell), 2D_0\big) \subset V.$$

Let us first give an overview of how to achieve this. Our strategy consists in choosing $D_0 = K + (c_1) + (c_2) + (c_3)$, where K is an effective canonical divisor, and the c_i are cusps, thus for us $d_0 = 2g+1$ exactly. First, we compute the $(g+2)$-dimensional space

$$V_2 = H^0\big(X_1(\ell), \Omega_1(c_1 + c_2 + c_3)\big).$$

This space is the direct sum of all the cusp forms of weight 2 and of the scalar multiples of Eisenstein series $e_{1,2}$ and $e_{1,3}$ of weight 2 vanishing at all cusps except c_1 and c_2 for $e_{1,2}$ and except c_1 and c_3 for $e_{1,3}$,

$$V_2 = S_2\big(\Gamma_1(\ell), \mathbb{C}\big) \oplus \mathbb{C}e_{1,2} \oplus \mathbb{C}e_{1,3} \subset M_2\big(\Gamma_1(\ell), \mathbb{C}\big).$$

[5] We have checked $p \leqslant 3$ is very often sufficient, and $p \leqslant 7$ is enough for all levels $\ell \leqslant 61$, except for $\ell = 37$ in which case we had to go up to $p = 19$.

The point of this is that by picking a rational cusp form $f_0 \in S_2\big(\Gamma_0(\ell), \mathbb{Q}\big)$, we obtain an isomorphism

$$\begin{array}{ccc} V_2 & \xrightarrow{\sim} & H^0\big(X_1(\ell), K + c_1 + c_2 + c_3\big) \\ f & \longmapsto & \dfrac{f}{f_0} \end{array},$$

where K is the divisor of the differential 1-form over $X_1(\ell)$ associated to the cuspform f_0, which is indeed an effective canonical divisor. Now by [KM04], lemma 2.2, the map

$$\begin{array}{ccc} V_2^{\otimes 3} & \longrightarrow & H^0\big(X_1(\ell), 3(K + c_1 + c_2 + c_3)\big) \\ f_1 \otimes f_2 \otimes f_3 & \longmapsto & \dfrac{f_1 f_2 f_3}{f_0^3} \end{array}$$

is surjective. We may thus choose V to be the image of the multiplication map

$$\begin{array}{ccc} V_2^{\otimes 3} & \longrightarrow & M_6\big(\Gamma_1(\ell), \mathbb{C}\big) \\ f_1 \otimes f_2 \otimes f_3 & \longmapsto & f_1 f_2 f_3 \end{array}.$$

In this framework, the subspace W_0 representing $0 \in J_1(\ell)$ is the image of the map

$$\begin{array}{ccc} V_2^{\otimes 2} & \longrightarrow & M_6\big(\Gamma_1(\ell), \mathbb{C}\big) \\ f_1 \otimes f_2 & \longmapsto & f_1 f_2 f_0 \end{array}.$$

From now on, we will implicitly identify weight-6 modular form spaces with the corresponding modular function spaces obtained by dividing by f_0^3.

We represent the weight-6 forms by their q-expansions at each cusp[6]. The modular curve $X_0(\ell)$ has exactly two cusps, namely $\Gamma_0(\ell)\infty$ and $\Gamma_0(\ell)0$, whereas the modular curve we're interested in, $X_1(\ell)$, has exactly $\ell - 1$ cusps, half of which lie above $\Gamma_0(\ell)\infty$ while the other half lie above $\Gamma_0(\ell)0$. We call the former cusps above ∞ and the latter cusps above 0. The cusps above 0 are all rational, whereas the cusps above ∞ make up a single Galois orbit. Now, the diamond operators $\langle d \rangle$, $d \in (\mathbb{Z}/\ell\mathbb{Z})^*$, which correspond to the action of the quotient goup $\Gamma_0(\ell)/\Gamma_1(\ell) \simeq (\mathbb{Z}/\ell\mathbb{Z})^*$, orbit the cusp $\Gamma_1(\ell)\infty$ onto the cusps above ∞, and the cusp $\Gamma_1(\ell)0$ onto the cusps above 0. Moreover,

[6]We could also have represented forms by their q-expansions at ∞ only, but we think using q-expansions at various cusps is better for numerical stability. Also we'll later need to be able to evaluate the forms at various points of the modular curve, hence it is better to know the q-expansions at various places.

the Fricke operator W_ℓ swaps $\Gamma_1(\ell)\infty$ and $\Gamma_1(\ell)0$. We know how the Fricke operator acts on newforms of weight 2 (cf subsection 3.1 on the periods), and on Eisenstein series (cf next subsection 3.3). Besides, all the forms we are dealing with with have characters, so that the action of the diamond operators $\langle d\rangle$ on their q-expansions boils down to multiplying by the value of their character at d. Using these two kinds of operators, we thus get the q-expansions of the newforms and of the Eisenstein series at all cusps from their q-expansions at ∞.

3.3 Finding the appropriate Eisenstein series

We now explain how to choose the Eisenstein series $e_{1,2}$ and $e_{1,3}$. Let us first review some facts about Eisenstein series of weight 2 in general (not necessarily prime) level N. From [DS05], chapter 4, we know that the Eisenstein subspace of $M_2\big(\Gamma_1(N),\mathbb{C}\big)$ has a basis formed of the Eisenstein series

$$G_2^{\psi,\varphi}(\tau)=\sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1}\psi(r)\overline{\varphi}(s)\sum_{\substack{(c,d)\in\mathbb{Z}^2\\ c\equiv rv \bmod N\\ d\equiv s+tv \bmod N}}\frac{1}{(c\tau+d)^2},$$

where ψ and φ are Dirichlet characters not both trivial, of the same parity, and of respective conductors u and v such that $uv=N$ exactly. We furthermore have the q-expansion at ∞

$$E_2^{\psi,\varphi}(\tau)=-\mathbb{1}_{u=1}\frac{1}{2}\sum_{a=0}^{v-1}\varphi(a)a\left(\frac{a}{v}+1\right)+2\sum_{n=1}^{+\infty}\left(\sum_{\substack{m>0\\ m|n}}\psi(n/m)\varphi(m)m\right)q^n,$$

where $E_2^{\psi,\varphi}$ is the normalisation of $G_2^{\psi,\varphi}$ defined by the relation

$$G_2^{\psi,\varphi}=\frac{-4\pi^2 g(\overline{\varphi})}{v^2}E_2^{\psi,\varphi},$$

and where $g(\cdot)$ denotes the Gauss sum of a Dirichlet character. Also, $G_2^{\psi,\varphi}\in M_2\big(\Gamma_1(N),\psi\varphi\big)$ has character $\psi\varphi$, where $\psi\varphi$ is seen as a Dirichlet character modulo N.

Consequently, in the case when $N=\ell$ is prime, we are left with only two cases, namely $G_2^{\chi,1}$ and $G_2^{1,\chi}$, where χ is a nontrivial even Dirichlet character

modulo ℓ. Both have character χ, and $G_2^{\chi,1}$ vanishes at ∞ while $G_2^{1,\chi}$ does not.

We easily check the formula

$$G_2^{\psi,\varphi}(\tau) = \sum_{(c,d)\in\mathbb{Z}^2} \frac{\psi(c)\overline{\varphi}(d)}{(vc\tau+d)^2},$$

from which it is clear that

$$W_N G_2^{\psi,\varphi} = \frac{u}{v}\psi(-1)G_2^{\overline{\varphi},\overline{\psi}},$$

and thus

$$W_N E_2^{\psi,\phi} = \frac{g(\psi)}{g(\overline{\varphi})}\frac{v}{u}\psi(-1)E_2^{\overline{\phi},\overline{\psi}}.$$

We construct Eisenstein series $e_{1,2}$ and $e_{1,3}$ as linear combinations of the $E_2^{\chi,1}$'s and the $E_2^{1,\chi}$'s, because they have nicer q-expansions than their G-counterparts. First, we choose the cusps c_1, c_2 and c_3 to be[7] $c_1 = \Gamma_1(\ell)0$, $c_2 = \langle 2\rangle c_1$, and $c_3 = \langle 3\rangle c_1$, so that they are all defined over $\mathbb{Q}$[8]. Next, we have from the above formulae

$$W_\ell E_2^{\chi,1} = \frac{g(\chi)}{\ell}E_2^{1,\overline{\chi}} \qquad \text{and} \qquad W_\ell E_2^{1,\chi} = \frac{\ell}{g(\overline{\chi})}E_2^{\overline{\chi},1},$$

from which we read that $E_2^{\chi,1}$ vanishes at the cusps above ∞ but not at the cusps above 0, while the opposite stands true for $E_2^{1,\chi}$. Consequently we construct $e_{1,2}$ and $e_{1,3}$ as linear combinations of the $E_2^{\chi,1}$ only. Now, it follows easily from the orthogonality relations between Dirichlet characters that the Eisenstein series

$$e_{1,2} = \sum_{\substack{\chi \text{ even}\\ \chi\neq 1}} \frac{1-\chi(2)}{g(\chi)\displaystyle\sum_{a=0}^{\ell-1}\overline{\chi}(a)a\left(\frac{a}{\ell}+1\right)}E_2^{\chi,1}$$

[7] These are all distinct as $\ell \geqslant 11$.

[8] This way, as the canonical divisor K is Galois-invariant since it is the divisor of $f_0 \in S_2\big(\Gamma_0(\ell),\mathbb{Q}\big)$, whose q-expansion at 0 is thus easily proved to be rational, our divisor D_0 used to run K. Khuri-Makdisi algorithms will be Galois-invariant, yielding a good behaviour with respect to the Galois action.

and

$$e_{1,3} = \sum_{\substack{\chi \text{ even} \\ \chi \neq 1}} \frac{1-\chi(3)}{g(\chi) \displaystyle\sum_{a=0}^{\ell-1} \overline{\chi}(a) a \left(\frac{a}{\ell}+1\right)} E_2^{\chi,1}$$

meet the requirements, that is to say $e_{1,2}$ vanishes at all cusps but c_1 and c_2, and $e_{1,3}$ vanishes at all cusps but c_1 and c_3.

3.4 Reducing the rough approximations of the torsion divisors

We have to reduce the divisors D_k^{big}, $k = 1, 2$. We describe below an algorithm to reduce a general, null-degree divisor

$$D^{\text{big}} = \sum_n \nu_n \big((P'_n) - (P_n)\big),$$

where the $\nu_n \in \mathbb{Z}$ are large integers, that is to say to compute the subspace W_D representing an effective divisor D of degree d_0 such that $D - D_0 \sim D^{\text{big}}$. This algorithm is to be used in parallel on the two divisors D_1^{big} and D_2^{big}, and we will denote by D_1^{crude} and D_2^{crude} the resulting reduced divisors.

For this we use K. Khuri-Makdisi's algorithms [KM04] [KM07]. These algorithms can only be input effective divisors D of degree d_0 exactly, by computing subspaces

$$W_D = H^0\big(X_1(\ell), 3D_0 - D\big) \subset V = H^0\big(X_1(\ell), 3D_0\big)$$

using linear algebra.

We first rearrange[9] the sum defining D^{big} into the form

$$\sum_i N_i \sum_{n=1}^{2g} m_{i,n} \big((P'_n) - (P_n)\big),$$

where the N_i and the $m_{i,n}$ are integers such that $\sum_{n=1}^{2g} |m_{i,n}| = d_0$ for each i and $|m_{i,n}| \leqslant 2$. We then input the subsums $\sum_{n=1}^{2g} m_{i,n}\big((P'_n) - (P_n)\big)$ for each i separately as follows. Letting

$$(Q'_n, Q_n) = \begin{cases} (P'_n, P_n) \text{ if } m_{i,n} \geqslant 0, \\ (P_n, P'_n) \text{ if } m_{i,n} < 0, \end{cases}$$

[9]This may require padding with a few cusps, cf the divisor D_{padding} in the next subsection.

so that we have

$$\sum_{n=1}^{2g} m_{i,n}\big((P'_n) - (P_n)\big) = \sum_{n=1}^{2g} |m_{i,n}|\big((Q'_n) - (Q_n)\big),$$

we compute the subspaces

$$W = H^0\left(X_1(\ell), 3D_0 - \sum_{n=1}^{2g} |m_{i,n}|Q_n\right) \subset V$$

and

$$W' = H^0\left(X_1(\ell), 3D_0 - \sum_{n=1}^{2g} |m_{i,n}|Q'_n\right) \subset V$$

by linear algebra, which is possible since we can evaluate the forms in the basis of V and their derivatives[10] at the points Q_n, Q'_n by using their q-expansions at the closest cusps. Our assumption that $\sum_{n=1}^{2g} |m_{i,n}| = d_0$ ensures we are inputting divisors of the correct degree d_0. Next, we use K. Khuri-Makdisi's algorithm to "subtract" these subspaces, meaning we find the subspace

$$W_{D_i} = H^0\big(X_1(\ell), 3D_0 - D_i\big) \subset V,$$

where D_i is an effective divisor of degree d_0 such that

$$D_i - D_0 \sim \sum_{n=1}^{2g} |m_{i,n}|\big((Q'_n) - (Q_n)\big).$$

We then use K. Khuri-Makdisi's algorithm in a fast exponentiation pattern in order to compute

$$W_{D_{i,N_i}} = H^0\big(X_1(\ell), 3D_0 - D_{i,N_i}\big) \subset V$$

where

$$D_{i,N_i} - D_0 \sim N_i(D_i - D_0),$$

and finally "Makdisi-sum" over i so as to get the subspace

$$W_D = H^0\big(X_1(\ell), 3D_0 - D\big) \subset V,$$

[10]As we required that $|m_{k,i,n}| \leqslant 2$, we have 0th- and 1st-order derivatives only to evaluate, which we think ensures better numerical stability.

where

$$D - D_0 \sim \sum_{i=1}^{j} (D_{i,N_i} - D_0).$$

We then indeed have

$$D - D_0 \sim \sum_i N_i \sum_{n=1}^{2g} m_{i,n}\big((P'_n) - (P_n)\big).$$

On a final note, we would like to point out that these computations can easily be parallelised, first by processing the divisors D_1^{big} and D_2^{big} in parallel of course, but also by processing the subblocks indexed by i in parallel too.

3.5 Refining the torsion divisors

We use Newton iteration in order to refine the two previously-computed crude approximations $D_k^{\text{crude}} - D_0$, $k = 1, 2$, of ℓ-torsion divisors into very-high-accuracy approximations $D_k^{\text{fine}} - D_0$ of these ℓ-torsion divisors. More precisely, we Newton-iterate the equation

$$\ell(D - D_0) \sim 0.$$

However, our divisors are represented in Makdisi form, that is to say by a subspace $W_D \subset V$. We thus need coordinate charts which are compatible with this representation. We need one chart φ from a neighbourhood of $0 \in \mathbb{C}^g$ to a neighbourhood of $0 \in J_1(\ell)(\mathbb{C})$ in order to be able to adjust the divisor we are working on, and another chart ψ from a neighbourhood of $0 \in J_1(\ell)(\mathbb{C})$ to $\mathbb{C}^g$ so as to check how far from linearly equivalent to zero ℓ times the divisor we are working on is.

First, pick g cusps $c_1, \cdots, c_g$. For each of these cusps, we have an analytic map, the "q-coordinate" around c_i

$$\kappa_i \colon \mathbb{E} \longrightarrow X_1(\ell)(\mathbb{C}),$$

where $\mathbb{E}$ stands for the open unit disk in $\mathbb{C}$, which maps 0 to the cusp c_i and which is a local diffeomorphism. Next, choose g complex numbers $q_1, \cdots, q_g$ of small moduli, so that each point $P_i = \kappa_i(q_i)$ is close to the cusp c_i. Also, initialise another vector of g complex numbers $\delta q_1, \cdots, \delta q_g$ to 0. Denoting

by P_i' the points $\kappa_i(q_i+\delta q_i)$, our first chart is then

$$\begin{array}{rccccc}\varphi\colon & U\subset\mathbb{E}^g & \xrightarrow{\prod\kappa_i} & \big(X_1(\ell)(\mathbb{C})\big)^g & \longrightarrow & J_1(\ell)(\mathbb{C}) \\ & (\delta q_i)_{1\leqslant i\leqslant g} & \longmapsto & (P_i')_{1\leqslant i\leqslant g} & \longmapsto & \left[\sum_{i=1}^g (P_i')-(P_i)\right]\end{array},$$

where U is a suitable neighbourhood of $0\in\mathbb{E}^g$. In other words, the perturbation we add to the divisor we are working on so as to make it ℓ-torsion is $\sum_{i=1}^g (P_i')-(P_i)$, where P_i has q-coordinate q_i and P_i' has q-coordinate $q_i+\delta q_i$. In order to have this work in Makdisi representation, we choose once and for all an effective divisor D_{padding} of degree d_0-g, and then we compute the subspaces

$$W=H^0\Bigg(X_1(\ell),3D_0-\underbrace{\sum_{i=1}^g P_i-D_{\text{padding}}}_{\text{degree } d_0}\Bigg)\subset V=H^0\big(X_1(\ell),3D_0\big)$$

and

$$W'=H^0\Bigg(X_1(\ell),3D_0-\underbrace{\sum_{i=1}^g P_i'-D_{\text{padding}}}_{\text{degree } d_0}\Bigg)\subset V=H^0\big(X_1(\ell),3D_0\big)$$

by linear algebra, exactly as in the previous part (we need to add the extra divisor D_{padding} so as to ensure we deal with effective divisors of the correct degree d_0). We then finally use K. Khuri-Makdisi's algorithm to compute the subspace $W\subset V$ representing the difference of these two divisors. We choose the coordinates q_i or the points P_i so that the differential of the map φ thus constructed is of full rank g, and not too ill-conditioned as well. Shrinking $U\subset\mathbb{E}^g$ if necessary, the map φ is therefore a diffeomorphism from $U\ni 0$ to a neighbourhood of $0\in J_1(\ell)(\mathbb{C})$, as desired.

Now that we know how to construct a small perturbation divisor in Makdisi form, we can add it to the divisor D_k^{crude} we want to refine into ℓ-torsion. We then multiply the result by ℓ, using K. Khuri-Makdisi's algorithms in a fast exponentation pattern. The result should thus be linearly equivalent to zero once the perturtation divisor, that is to say the vector $(\delta q_i)_{1\leqslant i\leqslant g}$, is suitably adjusted. In order to know where we are in the jacobian and to adjust the δq_i's accordingly, we need a coordinate chart working with Makdisi representation around $0\in J_1(\ell)(\mathbb{C})$.

Now there is an issue we have to overcome. A divisor class $x \in J_1(\ell)(\mathbb{C})$ is represented by a subspace $W_D = H^0\big(X_1(\ell), 3D_0 - D\big) \subset V$, where D is an effective divisor of degree $d_0 = 2g + 1$ such that $[D - D - D_0] = x$; but such a D is far from unique[11]! Thus, the first thing to do is to rigidify the representation W_D of x into a representation which depends on x only. To do this, we compute the sub-subspace

$$W_{D,\mathrm{red}} = H^0\big(X_1(\ell), 3D_0 - D - C_1\big) \subset W_D,$$

where C_1 is a fixed[12] effective divisor of degree $d_1 = 2d_0 - g$, so that $W_{D,\mathrm{red}}$ will generically be 1-dimensional by the Riemann-Roch theorem. Letting $s_D \in V$ be such that s_D spans $W_{D,\mathrm{red}}$ over $\mathbb{C}$, we know that the divisor of s_D is of the form

$$(s_D) = -3D_0 + D + C_1 + E_D,$$

where E_D is some effective divisor of degree g. As such, it generically sits alone in its linear equivalence class, again by the Riemann-Roch theorem. But on the other hand, if W_D and $W_{D'}$ both represent the same point $x \in J_1(\ell)(\mathbb{C})$, then $D \sim D'$, so that $E_D \sim E_{D'}$ as D_0 and C_1 are fixed. Consequently, we (generically) have $E_D = E_{D'}$, so that $W_D \mapsto E_D$ is the invariant we are looking for. In order to effectively compute E_D, we use a trick *à la* Makdisi: we first compute

$$s_D \cdot V = H^0\big(X_1(\ell), 6D_0 - D - C_1 - E_D\big),$$

after which we compute

$$H^0\big(X_1(\ell), 3D_0 - C_1 - E_D\big) = \{v \in V \mid vW_D \subset s_D \cdot V\},$$

all of this by linear algebra as in [KM04] and [KM07]. The divisor class of D is characterised by this subspace, but we would rather represent it by g complex coordinates than by a point in a grassmannian variety. For this, we fix another effective divisor[13] C_2 of degree $d_2 = d_0 + 1 - g$ chosen so that the

[11] To be precise, by the Riemann-Roch theorem, there is a whole $(g+1)$-dimensional projective space of such D's.

[12] It proves convenient to choose a divisor C_1 supported by cusps, so that the q-series are effortless to evaluate during the linear algebra part of the process, hence the notation C_1.

[13] Again, it is convenient to choose a divisor C_2 which is supported by cusps, for the same reasons as previously.

subspace $H^0\big(X_1(\ell), 3D_0 - C_1 - C_2 - E_D\big)$ of the previously computed space $H^0\big(X_1(\ell), 3D_0 - C_1 - E_D\big)$ is generically one-dimensional. When D varies, all of these one-dimensional subspaces are lines in the common space

$$V_{\mathrm{red},2} = H^0\big(X_1(\ell), 3D_0 - C_1 - C_2\big).$$

Summing up, we thus obtain a computable map (actually defined on an open dense subset only, due to the genericity assumptions)

$$\begin{array}{ccc} J_1(\ell)(\mathbb{C}) & \longrightarrow & \mathbb{P}(V_{\mathrm{red},2}) \simeq \mathbb{P}^g\mathbb{C} \\ W_D & \longmapsto & H^0\big(X_1(\ell), 3D_0 - C_1 - C_2 - E_D\big) \end{array}.$$

Furthermore, the divisor of a nonzero section in $H^0\big(X_1(\ell), 3D_0 - C_1 - C_2 - E_D\big)$ is of the form

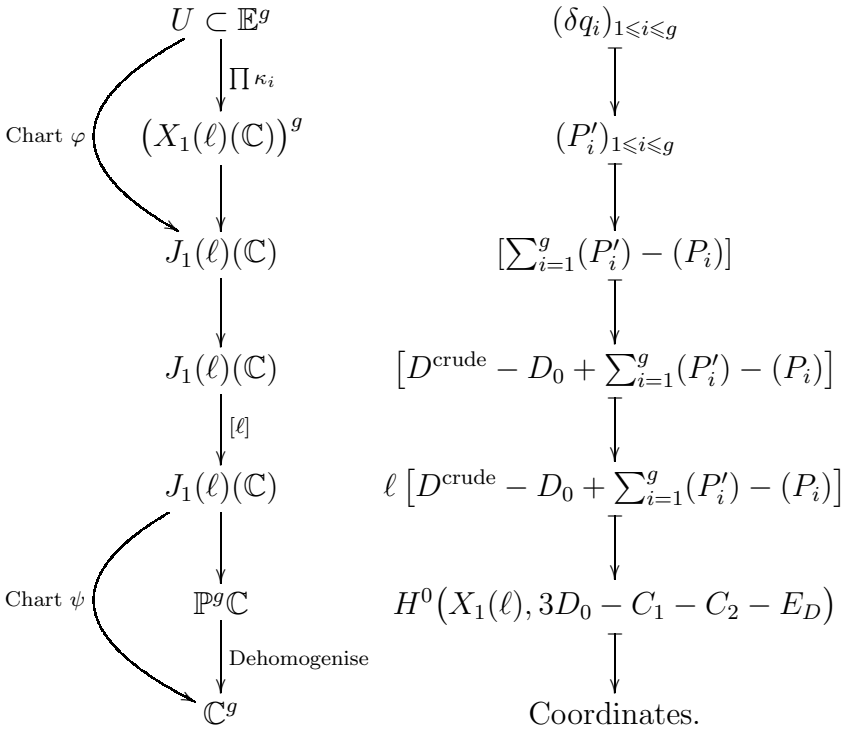
$$-3D_0 + C_1 + C_2 + E_D + R_D,$$

where R_D is a residual effective divisor of degree g. Consequently, the divisors having the same image as D are the divisors D' such that $E_{D'} \leqslant E_D + R_D$. This shows that this map has finite degree $\binom{2g}{g}$, hence is a local diffeomorphism as desired.

In order to have coordinates in $\mathbb{C}^g$ instead of $\mathbb{P}^g\mathbb{C}$, we can dehomogenise, for instance with respect to the coordinate the origin W_0 has the highest modulus at, in view of numerical stability. Restricting to divisor classes meeting the genericity assumptions and mapped to this inhomoegeneous chart domain, we finally obtain our chart ψ from a neighbourhood[14] of $0 \in J_1(\ell)(\mathbb{C})$ to $\mathbb{C}^g$.

[14]We choose C_1 and C_2 such that 0 is well-inside the domain of the chart ψ.

To sum up, the general picture is as follows :



Denoting the compositum of these maps by $\Phi\colon U \longrightarrow \mathbb{C}^g$, we are thus led to solve the equation

$$\Phi(\delta q_1, \cdots, \delta q_g) = \psi(W_0).$$

As Φ maps $\mathbb{C}^g$ to $\mathbb{C}^g$, we can use standard Newton iteration techniques for this. However, the map Φ is rather convoluted, so estimating its differential, which is necessary for Newton iteration, is quite difficult[15]. Therefore, we simply re-estimate this differential in each Newton iteration, by computing the growth rates in each direction

$$\frac{\Phi(\delta q_1, \cdots, \delta q_i + h, \cdots, \delta q_g) - \Phi(\delta q_1, \cdots, \delta q_g)}{h}, \quad 1 \leqslant i \leqslant g,$$

[15]Estimating this differential is actually possible: a computation using the implicit function theorem shows that it can be expressed as a sum over the zeroes of some function on $X_1(\ell)$. This sum can itself be rewritten as a contour integral using the residue theorem, but for this we need a contour on the compact Riemann surface $X_1(\ell)(\mathbb{C})$ which surrounds these zeroes with indices 1, and such a contour is very hard to compute.

where $h > 0$ decreases at the same rate as the distance $\|\Phi(\delta q_1, \cdots, \delta q_g) - \psi(W_0)\|$ (say, for instance, $h = \frac{1}{10}\|\Phi(\delta q_1, \cdots, \delta q_g) - \psi(W_0)\|$). It is easily checked that such a pattern still yields quadratic convergence. Of course, as Φ is expensive to compute with, the grow rates in each direction should be computed in parallel. Once $\|\Phi(\delta q_1, \cdots, \delta q_g) - \psi(W_0)\|$ has shrinked below the required accuracy, we can stop the iteration process.

3.6 Evaluating the torsion divisors

We need a Galois-equivariant function $\alpha \in \mathbb{Q}\big(J_1(\ell)\big)$ which can be efficiently evaluated at every point $x \in V_{f,\mathfrak{l}}$ given in Makdisi form. We then evaluate α at each nonzero point of $V_{f,\mathfrak{l}}$, and form the polynomial

$$F(X) = \prod_{\substack{x \in V_{f,\mathfrak{l}} \\ x \neq 0}} \big(X - \alpha(x)\big) \in \mathbb{Q}[X]$$

which defines the Galois representation $\rho_{f,\mathfrak{l}}$. In order to recognise its coefficients as rational numbers, we compute the continued fraction expansion of each of them until we find a huge term. Clearly, the lower the height of $F(X)$ the better, as it requires less precision in $\mathbb{C}$. This means one should use an evaluation function α whose divisor of poles (or zeroes) belongs to an as-"small"-as-possible class in the Néron-Severi group of $J_1(\ell)$.

The classical approach, used in [CEC3], [EdiC14], [Bos07] and [Zen12], consists in selecting a rational function ξ on $X_1(\ell)$ defined over $\mathbb{Q}$ and extending it to $J_1(\ell)$ by

$$\begin{array}{rccc} \Xi\colon & J_1(\ell) & \longrightarrow & \mathbb{C} \\ & \displaystyle\sum_{i=1}^{g} P_i - gO & \longrightarrow & \displaystyle\sum_{i=1}^{g} \xi(P_i) \end{array},$$

where $O \in X_1(\ell)(\mathbb{Q})$ is an origin for the Abel-Jacobi map. The divisor of the poles of Ξ is

$$(\Xi)_\infty = \sum_{Q \text{ pole of } \xi} \tau^*_{[Q-O]}\Theta,$$

where Θ is the theta divisor on $J_1(\ell)$ associated to the Abel-Jacobi map with origin O. We thus see that $(\Xi)_\infty$ is the sum of $\deg \xi$ translates of Θ, so that ξ should be chosen to have degree as low as possible. However, this degree is at least the gonality of $X_1(\ell)$, which is roughly g.

We introduce a radically different method, which can be used on the jacobian of any algebraic curve X, the genus of which we'll denote by g. Any point $x \in \mathrm{Jac}(X)$ can be written $[E_x - gO]$, where E_x is an effective divisor of degree g on X which is generically unique, and $O \in X$ is a fixed point. Let Π be a fixed divisor on X of degree $2g$. Then the space $H^0(X, \Pi - E_x)$ is generically 1-dimensional over $\mathbb{C}$, say spanned by $t_x \in \mathbb{C}(X)$. The divisor of t_x is of the form $(t_x) = -\Pi + E_x + R_x$, where R_x is a residual effective divisor of degree g on X, which is the image of E_x by the reflection

$$R_\Pi \colon \begin{array}{ccc} \mathrm{Pic}^g(X) & \longrightarrow & \mathrm{Pic}^g(X) \\ [E] & \longmapsto & [\Pi - E] \end{array} . \quad (\star)$$

Letting A and B be two points on X disjoint from the support of Π, we can then define

$$\alpha \colon \begin{array}{ccc} \mathrm{Jac}(X) & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \frac{t_x(A)}{t_x(B)} \end{array} .$$

This map is well-defined on a dense Zariski subset of $\mathrm{Jac}(X)$, and it is defined over $\mathbb{Q}$ if X, Π, A, B and O are defined over $\mathbb{Q}$. Moreover, it has a pole at $x \in \mathrm{Jac}(X)$ if and only if $[E_x - gO]$ or $[R_x - gO]$ are on the support of $\tau^*_{[B-O]}\Theta$. But $[R_x - gO]$ is the image of $[E_x - gO]$ by the involution $(\star)$, so finally we see[16] that the divisor of poles of α if the sum of only two translates of Θ, which is always much better than the Ξ used in the classical approach. It is even in some sense optimal, at least for a general curve, as by the Riemann-Roch theorem for abelian varieties (cf [HS00], theorem A.5.3.3), no nonconstant function on $\mathrm{Jac}(X)$ has a single translate of Θ as divisor of poles.

In order to use this on the modular curve $X_1(\ell)$, we choose $\Pi = 3D_0 - C_1 - C_2$, where C_1 and C_2 are divisors as in the previous subsection. If these divisors are chosen to be defined over $\mathbb{Q}$, then by construction of D_0, Π is also defined over $\mathbb{Q}$. It is then easy to compute t_x for $x = [D - D_0] \in J_1(\ell)$ represented in Makdisi form by $W_D \subset V$, as it is the exact same process as the one used in the previous subsection to define the coordinate chart ψ. Using the resulting map α on $V_{f,\mathrm{I}}$, we may thus hope to get a defining polynomial $F(X)$ of logarithmic height $g/2$ times less than if we had used the classical approach.

[16] We have $R_\Pi = \tau_\Pi \circ [-1]$, and $[-1]^*\Theta = \tau^*_{\mathcal{K}}\Theta$ is the translate of Θ by the image $\mathcal{K}$ of the canonical class, cf [HS00], theorem A.8.2.1.i.

3.7 Finding the Frobenius elements

After evaluating the torsion divisors by a suitable function, we get a polynomial $F(X) \in \mathbb{Q}[X]$ of degree $\ell^2 - 1$ whose decomposition field is the fixed field L by the kernel of the Galois representation. It is thus a Galois number field, and its Galois group over $\mathbb{Q}$ is embedded by the representation as a subgroup of $GL_2(\mathbb{F}_\ell)$. In order to completely specify the Galois representation, we would like to know what the Frobenius elements $\left(\frac{L/\mathbb{Q}}{p}\right)$ are similar to, for almost all[17] rational primes p. This can be used to get congruence relations modulo ℓ on the coefficients a_p of the cuspform f, by looking at the trace of the similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$.

For this, we adapt Tim and Vladimir Dokchitser's work [Dok10]. Although the Dokchitsers focus on the general case of identifying Frobenius elements classes as conjugation classes in the symmetric group $\mathfrak{S}_n$ acting on the roots of a defining polynomial, their work can easily be adapted to our needs. This yields the following result: denoting by $(a_i)_{1 \leqslant i < \ell^2}$ the roots of F in L, if $h(X) \in \mathbb{Z}[X]$ is a polynomial with integer coefficients, then for each similarity class $C \subset GL_2(\mathbb{F}_\ell)$, the resolvent polynomial

$$\Gamma_C(X) = \prod_{\sigma \in C} \left(X - \sum_{i=1}^{n} h(a_i)\sigma(a_i) \right)$$

lies in $\mathbb{Q}[X]$. Moreover, if p is a rational prime which divides none of the coefficients of F, so that the polynomials Γ_C are p-integral, which does not divide the discriminant of F, and such that the Γ_C's are pairwise coprime modulo p, then the image by the Galois representation of the Frobenius element $\left(\frac{L/\mathbb{Q}}{p}\right)$ lies in the similarity class C if and only if

$$\Gamma_C \left(\mathrm{Tr}_{\frac{\mathbb{F}_p[X]}{F(X)}/\mathbb{F}_p} h(a)a^p \right) = 0,$$

where a denotes the class of X in the quotient algebra $\mathbb{F}_p[X]/\big(F(X)\big)$. Furthermore, the polynomials Γ_C are pairwise coprime over $\mathbb{Q}$ for a generic choice of $h(X)$ amongst the polynomials of degree at most $\ell^2 - 2$ with coefficients in $\mathbb{Z}$.

[17] Clearly, we have to exclude $p = \ell$, as L is ramified at ℓ. We will shortly see that we actually have to exclude finitely many other primes as well.

We first start by computing the roots a_i to a very high precision in $\mathbb{C}$ using Newton iteration (note we already know them to a mildly high precision). Then, we compute complex approximations of the resolvents Γ_C by enumerating matrices in the similarity classes of $GL_2(\mathbb{F}_\ell)$. Finally, we recognise the coefficients of the resolvents as rationals, using our knowledge of an *a priori* multiple of their denominators, namely a common denominator for the coefficients of F to the cardinality of C times one plus the degree of h. In practice, the choice $h(X) = X^2$ has always worked, in that the resulting resolvents Γ_C we have computed have always been pairwise coprime over $\mathbb{Q}$, and actually, in all the computations we have run, they have even always remained coprime modulo p as long as p was reasonably large[18], say at least 10 decimal digits.

Once the resolvents are computed, it is easy to compute what Frobenius elements $\left(\frac{L/\mathbb{Q}}{p}\right)$ are similar to, and hence to deduce the coefficients of the cuspform f modulo $\mathfrak{l}$.

[18] As the primary goal of our computations is to find the coefficients a_p of the q-expansion of f modulo ℓ, the only case we are really interested in is the case in which p is extremely large, as naive methods compute a_p for small p in almost no time anyway.

4 Results

As the above algorithms compute the full Galois representation, we get results which are more complete than the ones from [Bos07]. For instance, picking $\ell = 19$ (which corresponds to genus 7), we can compute the Galois representation $\rho_{\Delta,19}$ modulo 19 associated to the newform

$$f = \Delta = q\prod_{n=1}^{+\infty}(1-q^n)^{24} = \sum_{n=1}^{+\infty}\tau(n)q^n$$

of weight 12, find the similarity class in $GL_2(\mathbb{F}_{19})$ of the images of Frobenius elements, and hence find the signs which were missing in the table on the very first page of [EC11] :

- The image of the Frobenius at $p = 10^{1000}+1357$ is similar to $\begin{bmatrix} 17 & 1 \\ 0 & 17 \end{bmatrix}$, therefore $\tau(10^{1000}+1357) \equiv -4 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+7383$ is similar to $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, therefore $\tau(10^{1000}+7383) \equiv +2 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+21567$ is similar to $\begin{bmatrix} 11 & 1 \\ 0 & 11 \end{bmatrix}$, therefore $\tau(10^{1000}+21567) \equiv +3 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+27057$ is similar to $\begin{bmatrix} 10 & 0 \\ 0 & 9 \end{bmatrix}$, therefore $\tau(10^{1000}+27057) \equiv 0 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+46227$ is similar to $\begin{bmatrix} 0 & 14 \\ 1 & 0 \end{bmatrix}$, therefore $\tau(10^{1000}+46227) \equiv 0 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+57867$ is similar to $\begin{bmatrix} 17 & 0 \\ 0 & 2 \end{bmatrix}$, therefore $\tau(10^{1000}+57867) \equiv 0 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+64749$ is similar to $\begin{bmatrix} 13 & 1 \\ 0 & 13 \end{bmatrix}$, therefore $\tau(10^{1000}+64749) \equiv +7 \bmod 19$,

- The image of the Frobenius at $p = 10^{1000}+68367$ is similar to $\begin{bmatrix} 14 & 0 \\ 0 & 5 \end{bmatrix}$, therefore $\tau(10^{1000} + 68367) \equiv 0 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+78199$ is similar to $\begin{bmatrix} 15 & 1 \\ 0 & 15 \end{bmatrix}$, therefore $\tau(10^{1000} + 78199) \equiv -8 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+128647$ is similar to $\begin{bmatrix} 0 & 8 \\ 1 & 0 \end{bmatrix}$, therefore $\tau(10^{1000} + 128647) \equiv 0 \bmod 19$.

Note that as Δ has weight 12, in each case, the determinant is congruent to $p^{11} \bmod 19$, as expected. The surprising number of occurences of non-semi-simple matrices — by the Chebotarev theorem, non-semi-simple matrices should occur with density about $1/\ell$ only — and of $\tau(p) \equiv 0 \bmod 19$ above can be explained by the fact that J. Bosman purposedly chose special values of p (cf [BosC7], section 7.4). For instance, for the few other first primes above 10^{1000}, we have computed the following:

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$
$10^{1000}+453$	$\begin{bmatrix} 15 & 0 \\ 0 & 10 \end{bmatrix}$
$10^{1000}+2713$	$\begin{bmatrix} 11 & 0 \\ 0 & 4 \end{bmatrix}$
$10^{1000}+4351$	$\begin{bmatrix} 6 & 0 \\ 0 & 4 \end{bmatrix}$
$10^{1000}+5733$	$\begin{bmatrix} 16 & 0 \\ 0 & 1 \end{bmatrix}$
$10^{1000}+10401$	$\begin{bmatrix} 0 & 15 \\ 1 & 8 \end{bmatrix}$
$10^{1000}+11979$	$\begin{bmatrix} 16 & 0 \\ 0 & 13 \end{bmatrix}$
$10^{1000}+17557$	$\begin{bmatrix} 0 & 5 \\ 1 & 11 \end{bmatrix}$
$10^{1000}+22273$	$\begin{bmatrix} 13 & 0 \\ 0 & 1 \end{bmatrix}$
$10^{1000}+24493$	$\begin{bmatrix} 14 & 0 \\ 0 & 10 \end{bmatrix}$
$10^{1000}+25947$	$\begin{bmatrix} 0 & 4 \\ 1 & 5 \end{bmatrix}$
$10^{1000}+29737$	$\begin{bmatrix} 0 & 12 \\ 1 & 7 \end{bmatrix}$
$10^{1000}+41599$	$\begin{bmatrix} 18 & 0 \\ 0 & 15 \end{bmatrix}$

This agrees with the Chebotarev theorem.

We have implemented the above algorithms in [SAGE], version 5.3, and have run them on PlaFRIM, the Bordeaux 1 university computing cluster. For $\ell = 19$, the computation times were as follows: computing the period

lattice, the q-expansion of the cuspforms and the Eisenstein series, and finally initialising K. Khuri-Makdisi's algorithms by computing the spaces V and W_0 took just a few minutes, inputting and simplifying the crude approximations of the two 19-torsion divisors took about one hour and a half (each, but they were processed in parallel), refining them by Newton iteration took a little less than 10 hours, computing all the points in the $\mathbb{F}_{19}$-plane spanned by them took about 40 minutes. We found a polynomial $F \in \mathbb{Q}[X]$ defining the representation, of degree $360 = 19^2 - 1$ and with a common denominator of 142 decimal digits, and finally, computing the resolvents $\Gamma_C(X)$ took 7 hours thanks to a massive parallelisation, after which deducing the similarity classes of the image of a Frobenius element at $p \approx 10^{1000}$ takes two-and-a-half hours. Overall, the whole computation thus lasted about 20 hours. We think these times could be reduced by an important constant factor if one rewrote in C language and optimised the core parts (that is to say, mainly the linear algebra over $\mathbb{C}$), but we have not had time to do it yet.

Complexity estimates and prospects

Clearly, the most time-consuming part of this algorithm is the arithmetic in the jacobian. K. Khuri-Makdisi's algorithms rely on linear algebra on matrices of size $O(g) \times O(g)$; as $g = O(\ell^2)$, this suggests a complexity of $\widetilde{O}(\ell^6)$ operations in $\mathbb{C}$ to compute the Galois representation. The experiments we have run seem to indicate the required precision in $\mathbb{C}$ is $O(\ell^2)$, so that we can estimate the general complexity of our method to be $\widetilde{O}(\ell^8)$ bit operations. We do not try to refine this estimate, because as we do not know any proven sharp bound on the height of the polynomial $F(X)$ defining the representation, we lack control on the precision.

We are currently running computations at level $\ell = 29$ (genus 22). Indeed, We had to skip $\ell = 23$ (genus 12) because the representation $\rho_{\Delta,23}$ degenerates. This phenomenon is related to Ramanujan-type congruences for $\tau(n)$ mod 23, cf the top of the fifth page of [EdiC1] and the first footnote in the introduction of this paper.

References

[AL78] Atkin, A. O. L.; Li, Wen Ch'ing Winnie, **Twists of newforms and pseudo-eigenvalues of W-operators**. Invent. Math. 48 (1978), no. 3, 221243.

[Bos07] Bosman, Johan, **On the computation of Galois representations associated to level one modular forms**. Available on arXiv.org at http://arxiv.org/abs/0710.1237

[Bos07a] Bosman, Johan, **A polynomial with Galois group $SL_2(\mathbb{F}_{16})$**. LMS J. Comput. Math. 10 (2007), 1461–1570.

[Bos11] Bosman, Johan, **Modular forms applied to the computational inverse Galois problem**. Available on arXiv.org at http://arxiv.org/abs/1109.6879

[BosC6] Bosman, Johan, **Computations with modular forms and Galois representations**. Chapter 6 of the book [EC11].

[BosC7] Bosman, Johan, **Polynomials for projective representations of level one forms**. Chapter 7 of the book [EC11].

[Buz00] Buzzard, Kevin, **On level-lowering for mod 2 representations**. Math. Res. Lett. 7 (2000), no. 1, 95–110.

[CEC3] Couveignes, Jean-Marc; Edixhoven, Bas, **First description of the algorithms**. Chapter 13 of the book [EC11].

[CouC12] Couveignes, Jean-Marc, **Approximating V_f over the complex numbers**. Chapter 12 of the book [EC11].

[CouC13] Couveignes, Jean-Marc, **Computing V_f modulo p**. Chapter 13 of the book [EC11].

[Cre97] Cremona, J. E., **Algorithms for modular elliptic curves**. Second edition. Cambridge University Press, Cambridge, 1997. vi+376 pp. ISBN: 0-521-59820-6.

[Dok10] Dokchitser, Tim and Vladimir, **Identifying Frobenius elements in Galois groups**. September 2010 preprint, to appear in Algebra and Number Theory.

[DS05] Diamond, Fred; Shurman, Jerry, **A first course in modular forms**. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005. xvi+436 pp. ISBN: 0-387-23229-X.

[EC11] **Computational aspects of modular forms and Galois representations**. Edited by Bas Edixhoven and Jean-Marc Couveignes, with contributions by Johan Bosman, Jean-Marc Couveignes, Bas Edixhoven, Robin de Jong, and Franz Merkl. Ann. of Math. Stud., 176, Princeton Univ. Press, Princeton, NJ, 2011.

[Edi92] Edixhoven, Bas, **The weight in Serre's conjectures on modular forms**. Invent. Math. 109 (1992), no. 3, 563–594.

[EdiC1] Edixhoven, Bas, **Introduction, main results, contexts**. Chapter 1 of the book [EC11].

[EdiC14] Edixhoven, Bas, **Computing the residual Galois representations**. Chapter 14 of the book [EC11].

[HS00] Hindry, Marc; Silverman, Joseph H., **Diophantine geometry - An introduction**. Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000. xiv+558 pp. ISBN: 0-387-98975-7; 0-387-98981-1.

[KM04] Khuri-Makdisi, Kamal, **Linear algebra algorithms for divisors on an algebraic curve**. Math. Comp. 73 (2004), no. 245, 333–357.

[KM07] Khuri-Makdisi, Kamal, **Asymptotically fast group operations on Jacobians of general curves**. Math. Comp. 76 (2007), no. 260, 2213–2239.

[Lan95] Lang, Serge, **Introduction to modular forms**. With appendixes by D. Zagier and Walter Feit. Corrected reprint of the 1976 original. Grundlehren der Mathematischen Wissenschaften, 222. Springer-Verlag, Berlin, 1995. x+261 pp. ISBN: 3-540-07833-9.

[Li03] Li, Tien-Yien, **Numerical solution of polynomial systems by homotopy continuation methods**. In F. Cucker, editor, Handbook of Numerical Analysis. Volume XI. Special Volume: Foundations of Computational Mathematics, pages 209–304. North-Holland, 2003.

[Rib94] Ribet, Kenneth A., **Report on mod ℓ representations of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)**. Motives (Seattle, WA, 1991), 639676, Proc. Sympos. Pure Math., 55, Part 2, Amer. Math. Soc., Providence, RI, 1994.

[SAGE] **SAGE mathematics software**. http://sagemath.org/

[Sch95] Schoof, Ren, **Counting points on elliptic curves over finite fields**. Les Dix-huitimes Journes Arithmtiques (Bordeaux, 1993). J. Thor. Nombres Bordeaux 7 (1995), no. 1, 219–254.

[Ste07] Stein, William, **Modular forms, a computational approach**. With an appendix by Paul E. Gunnells. Graduate Studies in Mathematics, 79. American Mathematical Society, Providence, RI, 2007. xvi+268 pp. ISBN: 978-0-8218-3960-7; 0-8218-3960-8.

[Zen12] Zeng, Jinxiang, **On the computation of coefficients of modular forms: the p-adic approach**. Available on arXiv.org at http://arxiv.org/abs/1211.1124